ARRT
Advanced Risk Reduction Tool

Presentation to the 1st Annual NASA
Office of Safety and Mission Assurance (OSMA)
Software Assurance Symposium (SAS)

Dr. Martin S. Feather
ARRT Center Initiative Lead*
Jet Propulsion Laboratory
California Institute of Technology

Martin.S.Feather@Jpl.Nasa.Gov
http://eis.jpl.nasa.gov/~mfeather

*Initiative began in 1999 with Dr. John Kelly as Lead

ARRT Heritage & Contributors

ARRT is inspired by, and based on
JPLer Steve Cornford's Defect Detection and Prevention (DDP)
and JPLer Tim Larson's Risk Balancing Profiles (RBP).

contributors (JPL)

John Kelly
Burt Sigal
James Eddingfield
Steve Cornford
Phil Daggett
Julia Dunphy
Roger Klemm

contributors

Jim Kiper (U. Miami, Ohio)
William Evanco (Drexel)
Steve Fickas (U. Oregon)
Martha Wetherholt (NASA Glenn)
Richard Hutchinson (Wofford, SC)

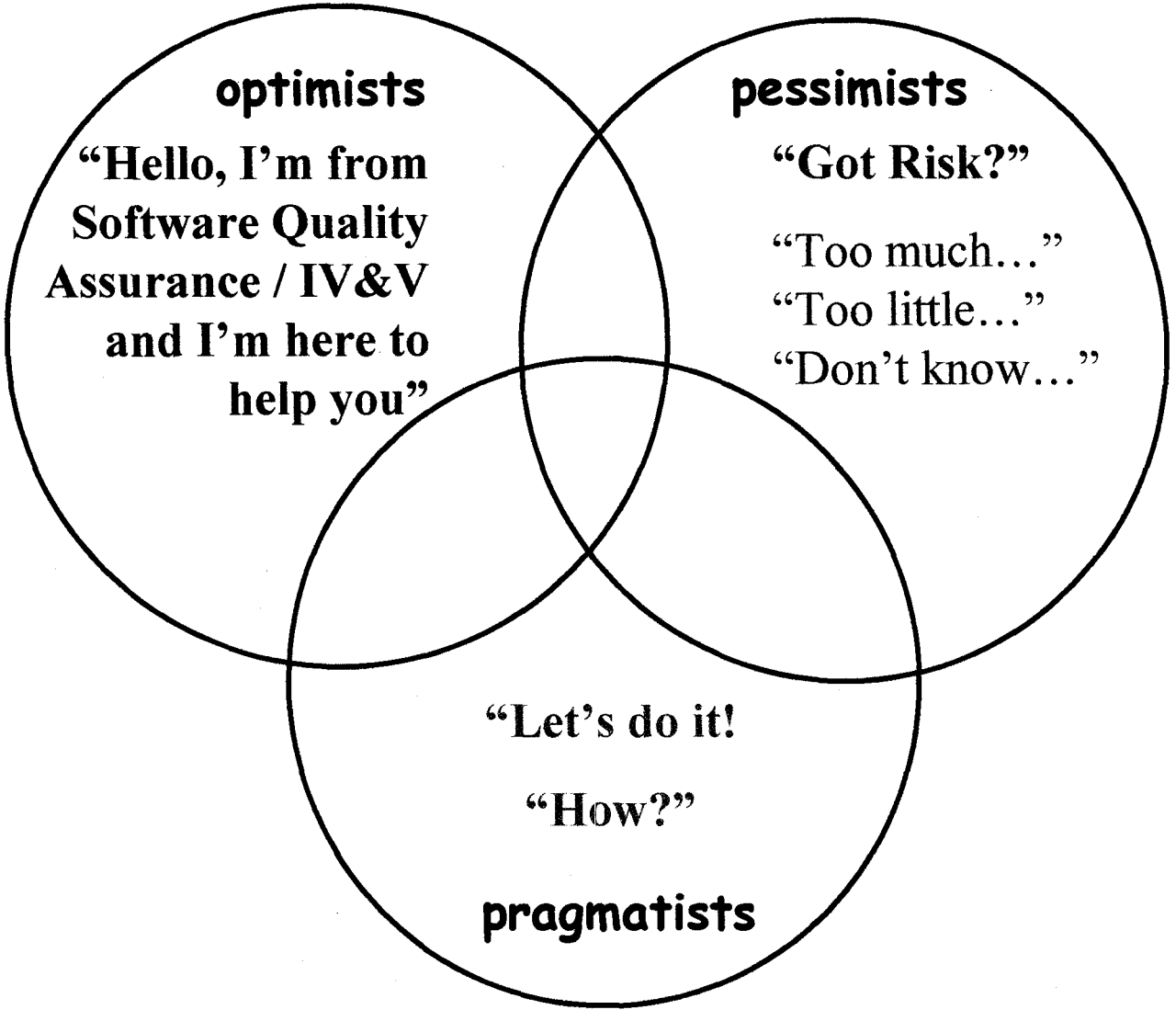
primary collaborators

Tim Menzies (U. British Columbia)
Tim Kurtz (NASA Glenn)
Hoh In (Texas A&M)

funding, management & guidance

NASA Code Q, NASA Goddard IV&V Facility
Siamak Yassini, Ken McGill, Marcus Fisher

The Universe of ARRT Customers



The Optimists "Hello, I'm from Software Quality Assurance / IV&V and I'm here to help you"

Many attendees of this symposium are likely to already believe in the net value of assurance activities, but optimism alone is not sufficiently contagious!

What is needed is the means to *quantitatively* assess the cost/benefit of assurance activities applied to specific projects. This will:

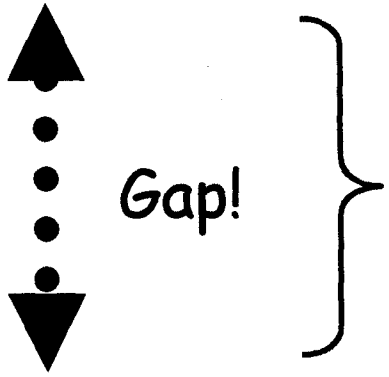
- be more convincing
- determine best use of limited resources
- identify alternatives (e.g., requirements to discard)

The Optimists

Cost/benefit data & reasoning has been applied to:

Individual activities, e.g., Regression testing [Graves et al, 1998].

Pairwise comparisons, e.g., "Peer reviews are more effective than function testing for faults of omission and incorrect specification" [Basili & Boehm, 2000].



ARRT performs quantitative cost/benefit calculation for *suite* of assurance activities applied to a specific project

Lifecycle process improvement, e.g., Quality, productivity and estimation gains from CMM-like process improvement [McGarry et al, 1998].

ARRT's Quantitative Cost/Benefit Model

Risk mitigations subdivided into

Preventions – prevent problems from appearing in the first place
e.g., training programmers → fewer coding errors
cost = performing prevention
benefit = reduction of risk likelihood

Detections – detect problems so that they can be corrected
e.g., unit testing → detects internal coding errors
cost = performing detection +
performing the repair (cost depends on when!)
benefit = reduction of risk likelihood

Alleviations – applied to decrease the severity of problems
e.g., robust coding → tolerant of out-of-bound input values
cost = performing alleviation
benefit = reduction of risk severity

Cost/Benefit – Simple Scenario

mistakes happen

Implementation phase

Requirements phase

Poorly written requirements

Use ARM to do Requirements Analysis ($)

Correct ambiguous requirements ($)

Low costs to analyze with ARM & correct flaws now

Programming errors

Misinterpret ambiguous requirements

assurance choices

Test phase

System tests, observed by spacecraft engineers($$)

Reimplement misinterpreted requirements ($$$)

Correct programming errors ($$)

High cost to reimplement requirements this late in development

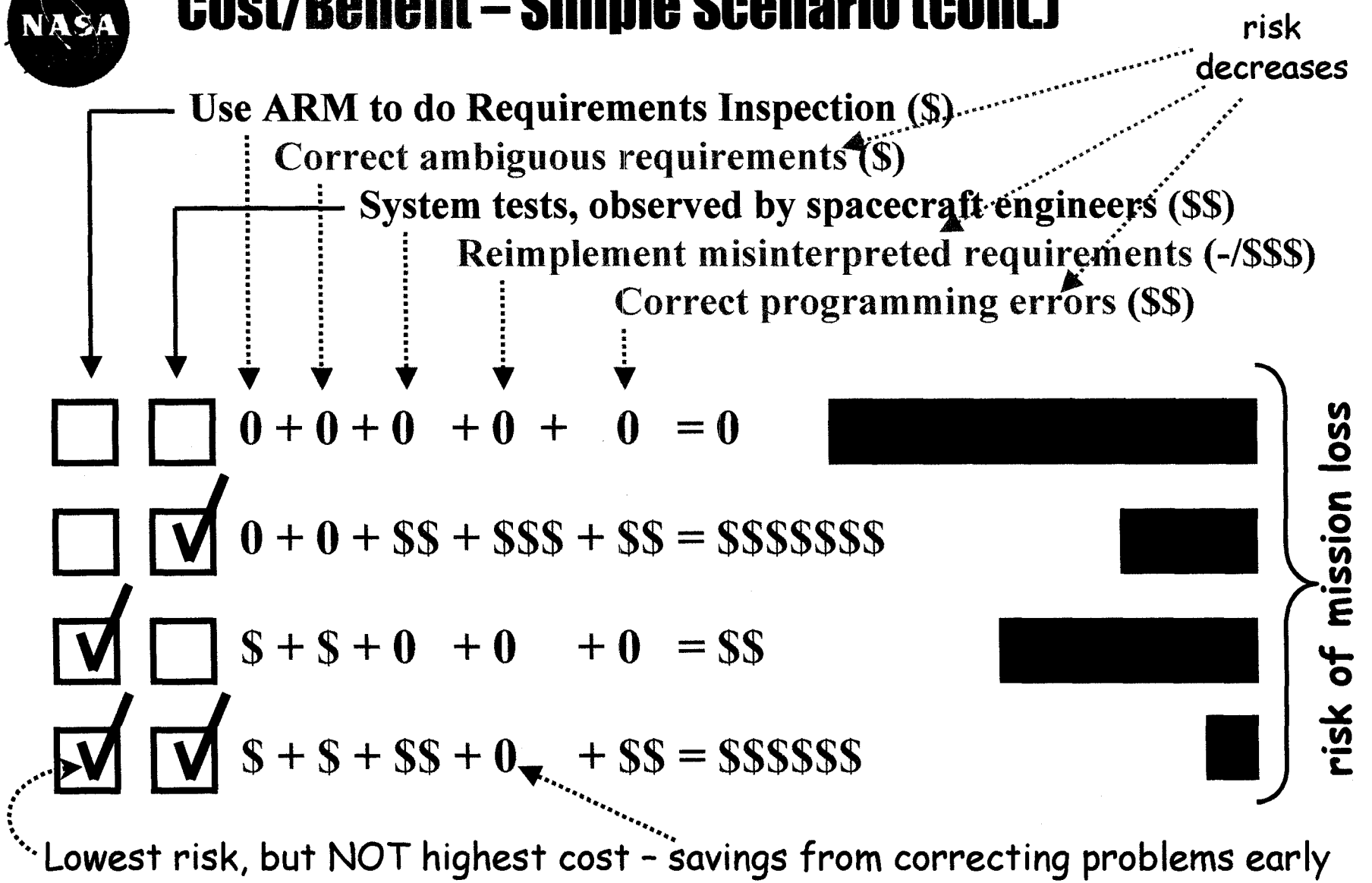
Operations phase

RISKS

Mission loss due to misinterpretation of requirements

Mission loss due to programming errors

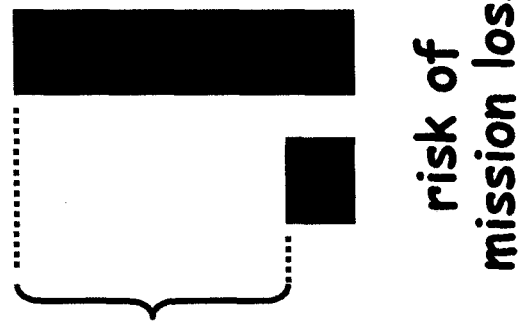
Cost/Benefit – Simple Scenario (cont.)



Return On Investment of Assurance/IV&V

☑ ☐ $ + $ + 0 + 0 + 0 = $$

☑ ☑ $ + $ + $$ + 0 + $$ = $$$$$$



Is it worth paying $$$$ to save this much risk?

Risk = loss of Requirements

If you are bold enough to value Requirements in the same unit of currency as costs of Mitigations, then you can calculate **Return On Investment (ROI)**

Valuation of Requirements can be difficult, e.g.,

- What is the value of discovering water on Mars?
- What is the value of returning a Mars sample to Earth?
- What is the value of an astronaut's life?

ARRT's Quantitative Cost/Benefit Model

Cost/benefit computations in ARRT

- Automatic
- Handle *suite* of assurance activities
- Permit data to be changed if we know better than standard estimates
- Distinguish development phases (requirements, design, ...)
- Distinguish preventions, detections and alleviations
- Combine with underlying risk computation model (see next section)

The Pessimists GOT RISK?

TOO MUCH **– use ARRT to plan how to reduce risk in a cost-effective manner.**

TOO LITTLE **– use ARRT to plan how to accept more risk in exchange for reduced cost and schedule, more functionality, etc.**

JUST RIGHT **– use ARRT to maintain a desired risk profile through the lifetime of the project.**

DON'T KNOW **– use ARRT to assess risk status.**

"Risk as a Resource" - Dr. Michael Greenfield [Greenfield, 1998]

ARRT's treatment of Risk– DDP & RBP concepts, specifically populated with software data

ARRT is inspired by, and based on
JPLer Steve Cornford's Defect Detection and Prevention (DDP)
and JPLer Tim Larson's Risk Balancing Profiles (RBP).

In particular, ARRT inherits DDP's Risk Model.

DDP is a *process* [Cornford et al, 2001]
supported by a custom *tool* [Feather et al, 2000a] for
quantitative risk management.

RBP is a *qualitative* risk management tool populated with
risk and risk mitigation data.

DDP & RBP merged [Feather et al, 2000b] into DDP

ARRT uses this merged combination of DDP & RBP

ARRT inherits DDP's Risk Model

DDP utilizes three trees of key concepts:

Requirements (what you want)

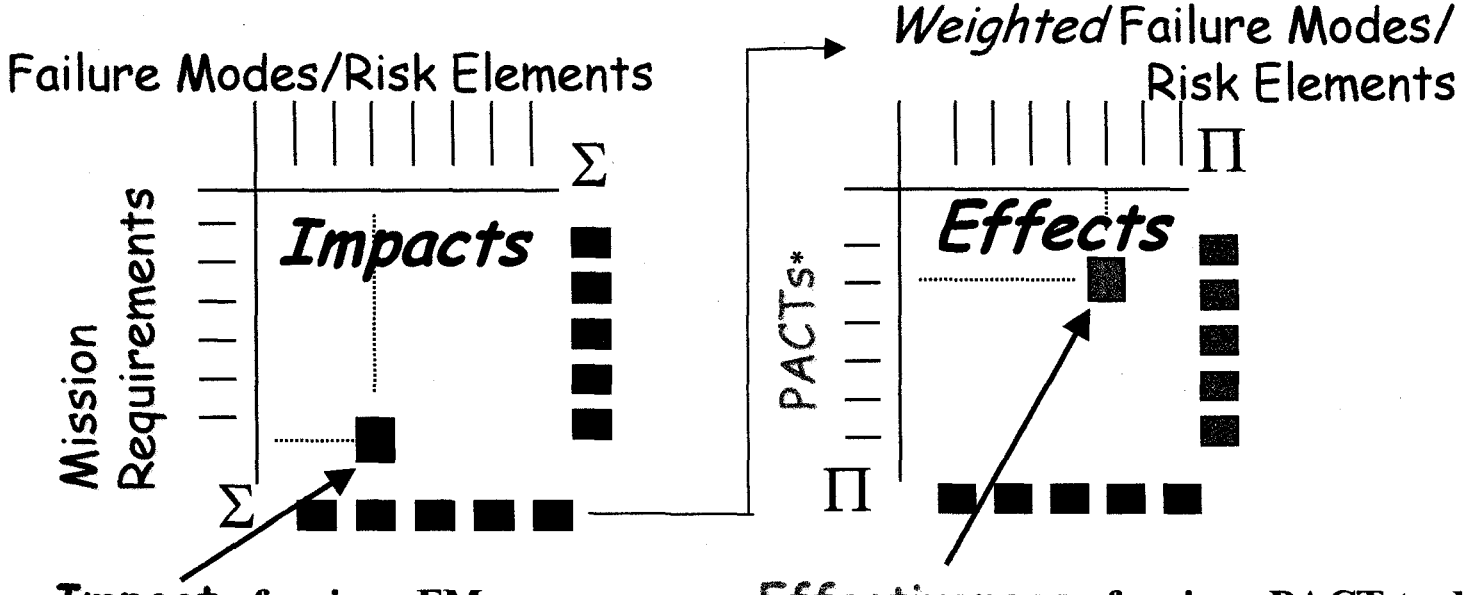
Failure Modes / Risk Elements (what can get in the way of requirements)

PACTs (what can mitigate risk)

and two matrices that connect those concepts:

Impacts (how much Requirement loss is caused by a FM)

Effectivenesses (how much a PACT mitigates a FM)



Impact of a given FM on a particular requirement

Effectiveness of a given PACT to detect, prevent or alleviate a particular FM

ARRT/DDP Computations & Visualizations

Information is derived from user-provided data via built-in computations, e.g.,

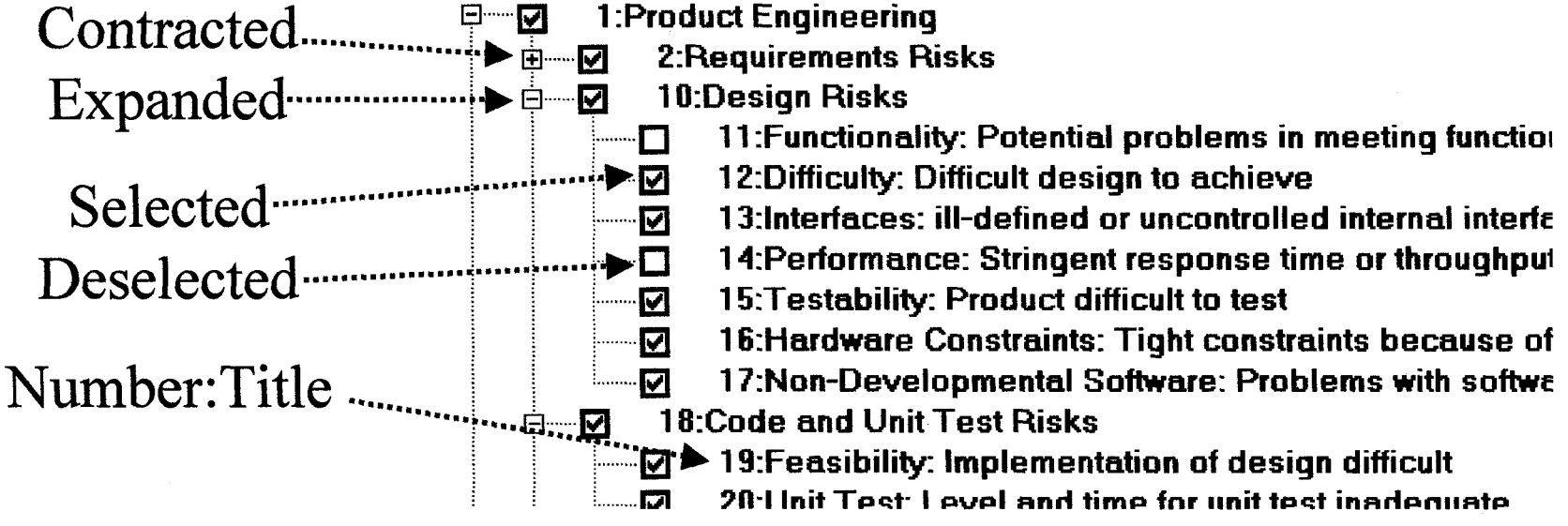
- FM's cumulative impact = FM.Likelihood * (Σ (R $\in$ Requirements) R.Weight * Impact(R, FM))

Information presented via cogent visualizations

- Bar charts
- Risk Region chart
- Stem-and-leaf plots
- Detailed view of properties of individual element

ARRT/DDP Trees

Taxonomies of Software Requirements / Risks / Risk Mitigations



Autonumbering: *linear* 1,2,… or *tree* 1, 1.1, 1.2, 1.2.1, …

ARRT/DDP Matrices

Effects (Mitigation x Risk)

		FMs						
		FMs						
		FMs	Stabilit		Clarity	Validit	Feasib	Pre
PACTs	PACTs	FoM\R	0.5	0.5	0.5	0.5	0.5	0.5
	Authori	2.95	0.1	0.1	0.1	0.1	0.1	0.3
	Identify	2.3						
	Mainta	0						
	Softwa	2.65						
	Implem	1.85	0.9	0.3	0.9	0.9	0.3	0.3
	Manag	0.15						
	Docum	1.65	0.3	0.9	0.9	0.1	0.3	0.3
	Peer	2.8	0.9	0.9	0.9	0.9	0.9	0.9

numbers supplied by experts and/or based on accumulated metrics

proportion of Risk reduced by Mitigation

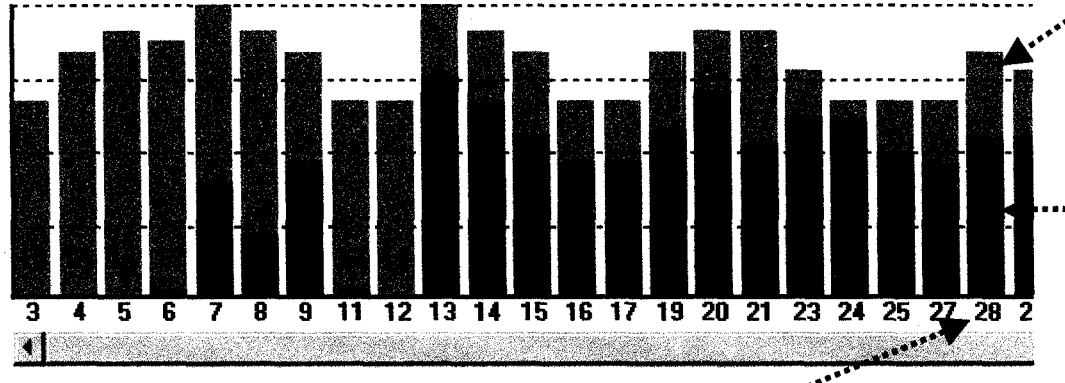
Impacts (Requirement x Risk):

proportion of Requirement loss if Risk occurs

ARRT/DDP Visualizations - Bar Charts

Risks bar chart

Unsorted – order matches leaf elements in Risk tree

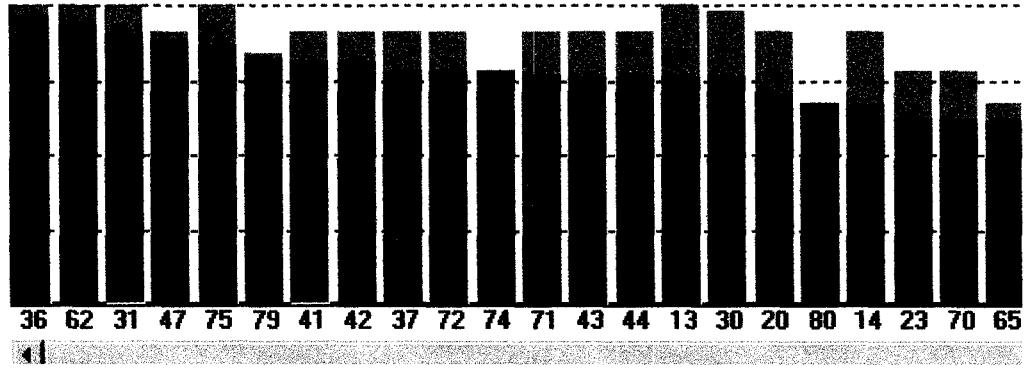


Item number in tree

Green: of this Risk's total Impact on Requirements, that *saved* by Mitigations

Red: of this Risks's total Impact on Requirements, that *remaining* despite Mitigations

Sorted – in decreasing order of remaining risk



Requirements bar chart – how much each is impacted

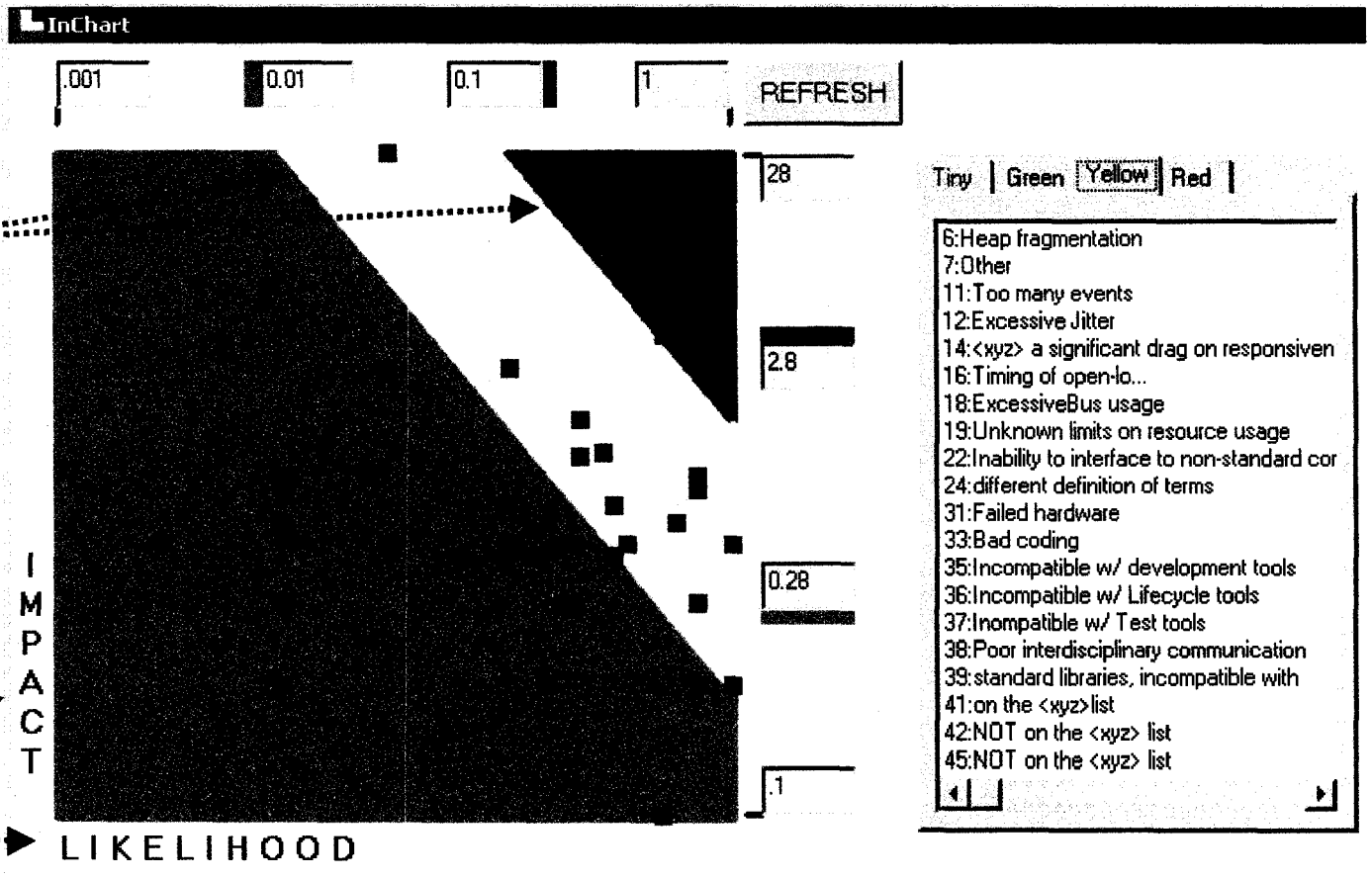
Mitigations bar chart – how much impact each is saving

ARRT/DDP Visualizations - Risk Region "InChart"

User defines risk levels demarking red/yellow/green/(tiny) risk regions

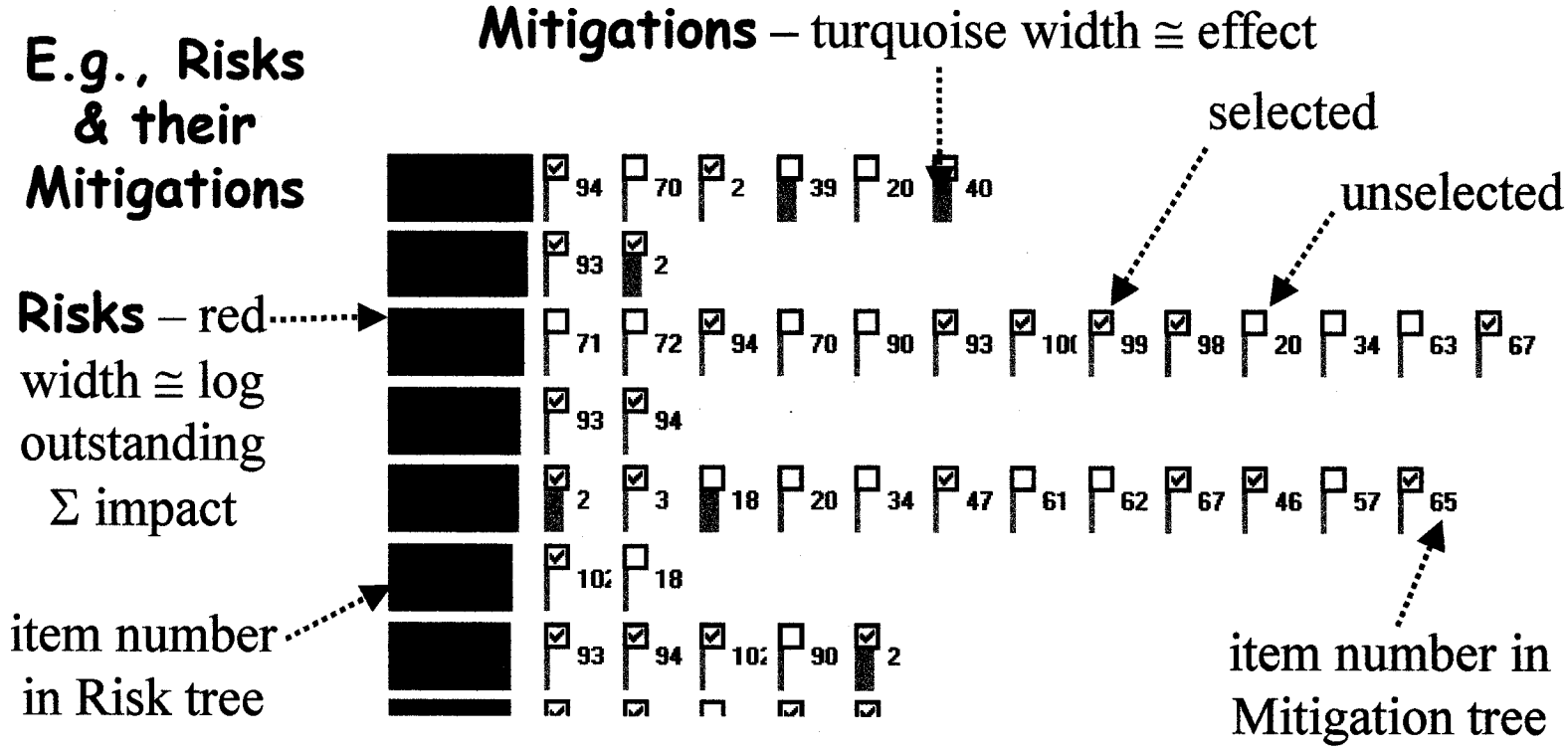
Log/Log scale: diagonal boundaries = risk contour lines

Conventional measure of risk as impact (severity) x likelihood.



ARRT/DDP Visualizations - stem-and-leaf(*) charts

Compact visualization of DDP's sparse matrices



(*) Tufte attributes these to John W. Tukey, "Some Graphical and Semigraphic Displays"
Their usage was introduced into RBP by D. Howard, extended further by us in DDP.

The Pragmatists

"Has it been used?"

"Where does the data come from?"

"How does it combine with software estimation & planning?"

"What about...?"

Focused study data: Software Assessment Exercise

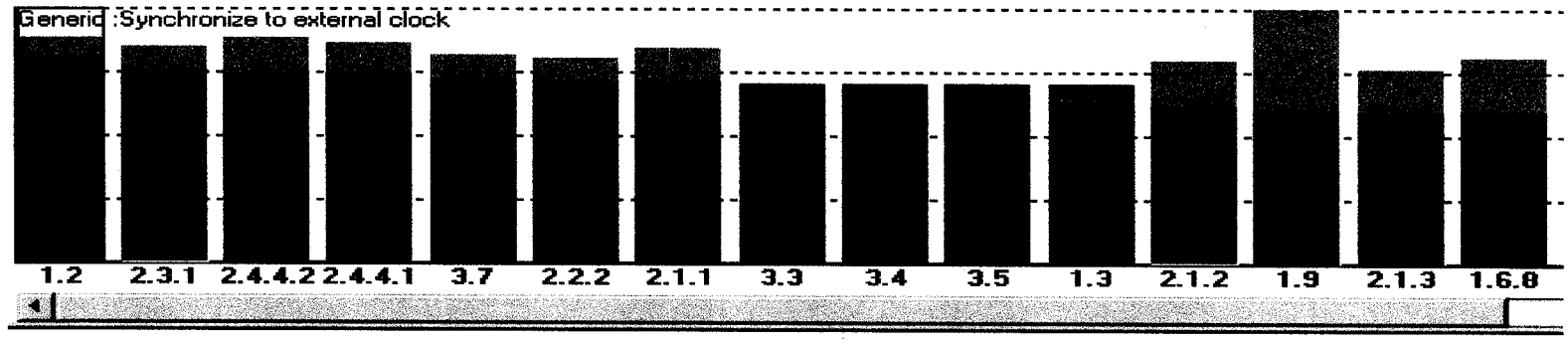
Steve Cornford, JPL + others

- Focus: code generation by [product name deliberately hidden]
  - Flight code of modest experiment
  - Flight code for future missions
- 15+ experts in 4 x 4-hour sessions, Sept 2000
  - [product] experts
  - Mission experts
  - Software experts (SQA, coders, …)
- Large information set
  - 47 Requirements (unprioritized)
  - 76 Risks (near-term mission-specific & futuristic)
  - 303 Mitigations (pre-populated with large set)
  - 107 Impacts
  - 223 Effects

Software Assessment Exercise – extract

Portions of the Requirements tree and bar chart

- 2.2.3:Comm IF's
  - 2.2.3.1:IEEE 1394
  - 2.2.3.2:RS-422 (etc)
  - 2.2.3.3:MIL STD 1553/1773
- 2.3:Data Handling
  - 2.3.1:Accomodate SW upgrades in flig
  - 2.3.2:Telemetry
    - 2.3.2.1:Uplink and downlink accour
      - 2.3.2.1.1:Uplink
      - 2.3.2.1.2:Downlink
  - 2.3.3:Storage
- 2.4:Fault Protection
  - 2.4.1:System level fault protection
  - 2.4.2:Code and Data separable
  - 2.4.3:Work around memory errors
  - 2.4.4:Autonomous failure recovery
    - 2.4.4.1:Due to external failures
    - 2.4.4.2:Due to Internal failures
- 3:Programmatic Requirements
  - 3.1:Budget = TBD$
  - 3.2:Deliver in 2003
  - 3.3:Use TBD developmental tools
  - 3.4:Use TBD lifecycle tools
  - 3.5:Use TBD test tools
  - 3.6:Utilize legacy code
  - 3.7:Link w/ other lanquaqes



Software Engineering Community Data

- **Risks**: Software Risk Taxonomy (SEI)
- **Mitigations**: two datasets:
  1. JPL's Risk Balance Profile of SQA actions
  2. Assurance activities from Ask Pete (NASA Glenn tool)
- **Effects**: cross-linkings of the above (Jim Kiper)
  1. Expert's best estimates of yes/no (Prof. J. Kiper)
  2. Experts' 1000+ best estimates of quantified effectiveness (Prof. J. Kiper & J. Eddingfield)

Note: **Requirements** are PROJECT SPECIFIC

Software Estimation & Planning data: ARRT – Ask Pete collaboration

see companion presentation in this symposium

Tim Kurtz, ⇨
Tim.Kurtz@grc.nasa.gov
SAIC/NASA Glenn Research Center
http://tkurtz.grc.nasa.gov/pete
Principal Investigator ⇨ Martha Wetherholt

Ask Pete runs to gather project characteristics, make first cut at suggested selection of risk mitigations.
Mitigation selection passed to ***ARRT***

ARRT runs to allow user to assess risk, provide costs, **customize to project** (add/remove risks, refine effect values, etc.), tune selection accordingly.
Revised mitigation selection returned to ***Ask Pete***

Ask Pete runs to generate final reports

ARRT - Tim Menzies collaboration

see companion presentation in this symposium

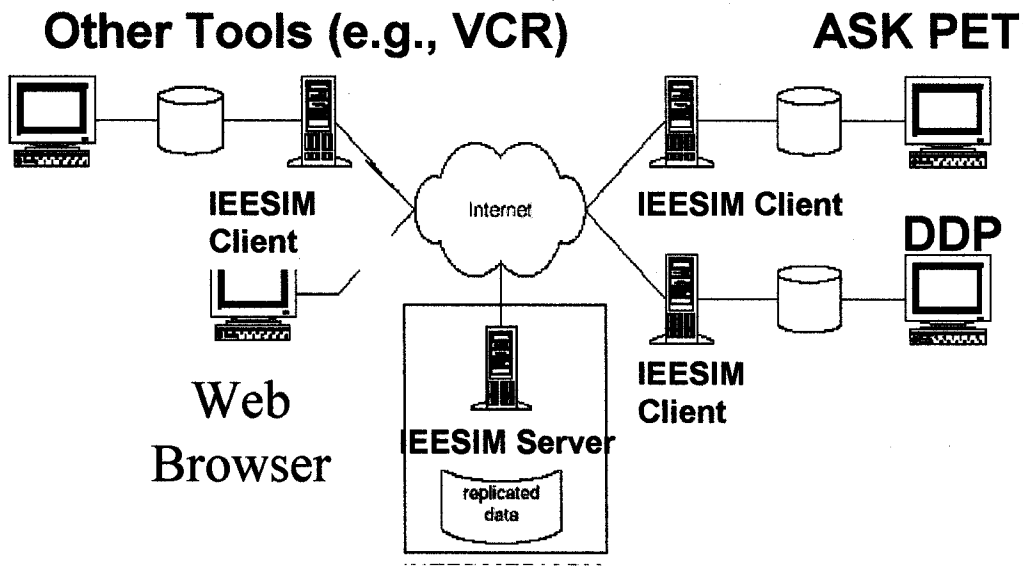
tim@menzies.com

Prof. Tim Menzies, U. British Columbia

Benefits to ARRT of collaboration

- **Optimization** – automated search for (near) optimal mitigations suites
  - Least risk for given cost
  - Least cost for given risk
- **Sensitivity analysis**
  - On which data values do the results hinge?
    - Scrutinize these values further
    - Identify points of leverage (e.g., problematic requirements; make-or-break decisions)
- **Retain human involvement**
- **Extend reasoning to more complex data**
  - Interactions: mitigations that induce risk (e.g., code changes to correct one bug may introduce other bugs)
  - Ranges / distributions of values (e.g., [0.1 – 0.3])

ARRT – Hoh In et al collaboration: IEESIM



Repository of project data

Insert & classify,
Search,
Retrieve,
Delete

Accessibility via the web

http://
www.cs.tamu.edu/
faculty/hohin/

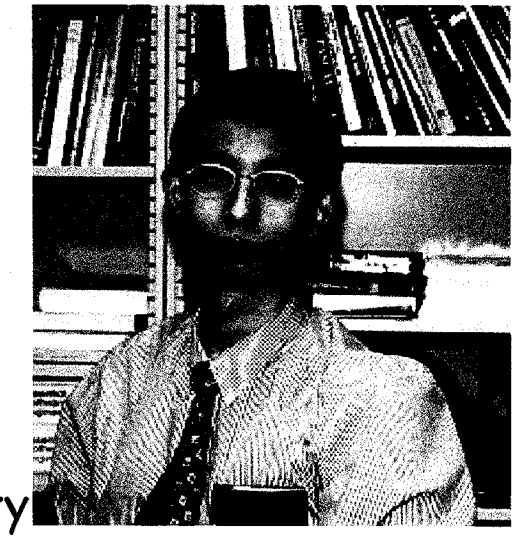
IEESIM

Integrated views (data schema) from local tool views

Exchangeable format based on XML

Extendable interfaces for additional tools

Shared Information Mediator



Prof. Hoh In, Texas A&M University

Hoh In et al – Visualized Conflict Resolution (VCR)

ARRT data passed to VCR. Purposes:

see Friday's demo at this symposium

[Hoh & Roy, 2001]

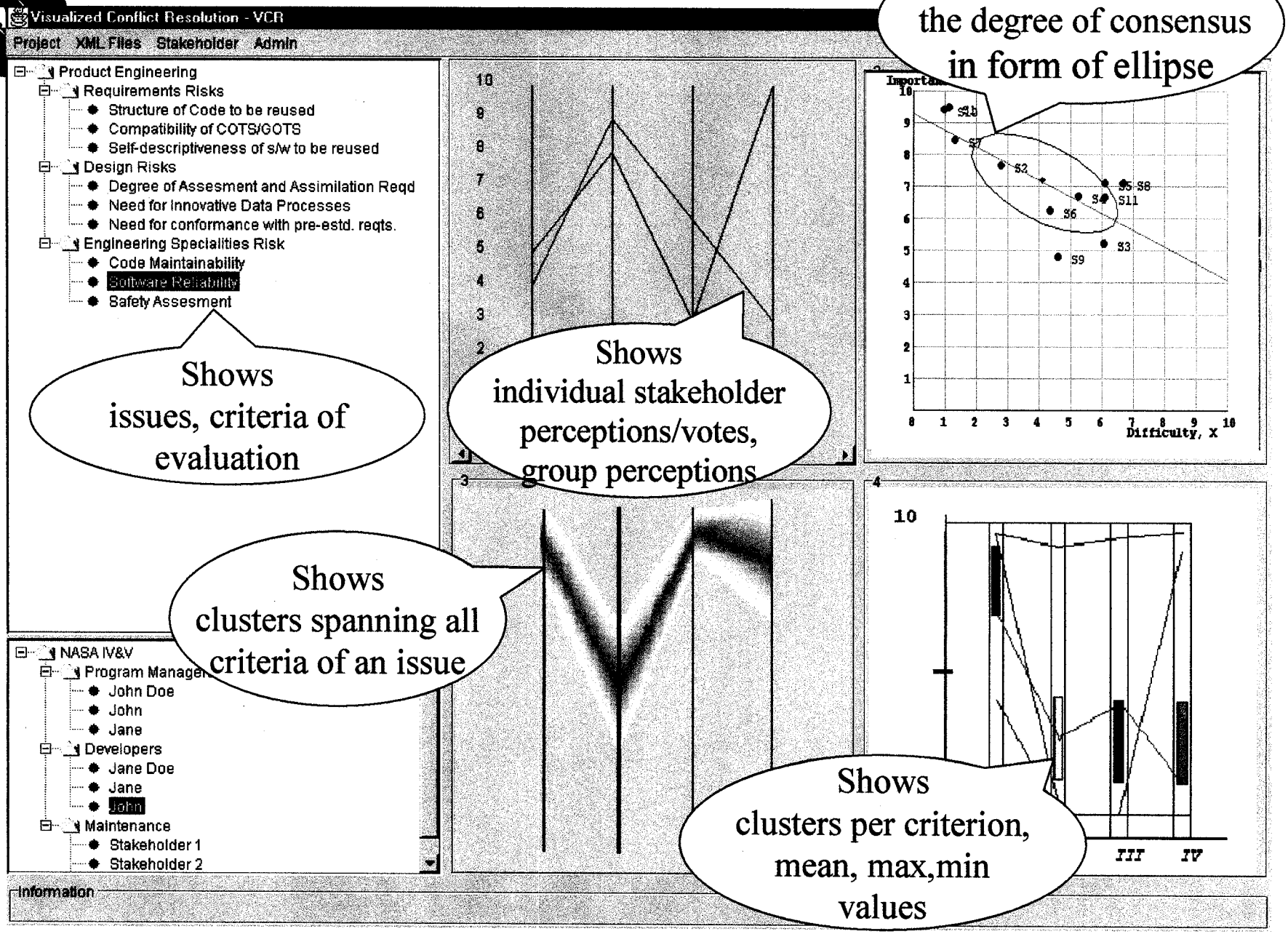
- **Sophisticated Visualization**
  - Intuitive graphical presentations of consensus, conflict trends.
  - Scalable and multi-dimension visualization.
- **Powerful Analysis Support**
  - Identify non-trivial interrelationships (Clustering).
  - Discover stakeholder decision rationales (Profiles).
  - Benefit-cost tradeoff analysis

XML adopted as standard medium of data exchange

Status: examples of both kinds of data transferred & visualized

Hoh's visualization work motivated inclusion of the green/yellow/red Risk chart capability into ARRT - slide 18

Hoh In et al – Visualized Conflict Resolution (VCR)



Shows the degree of consensus in form of ellipse

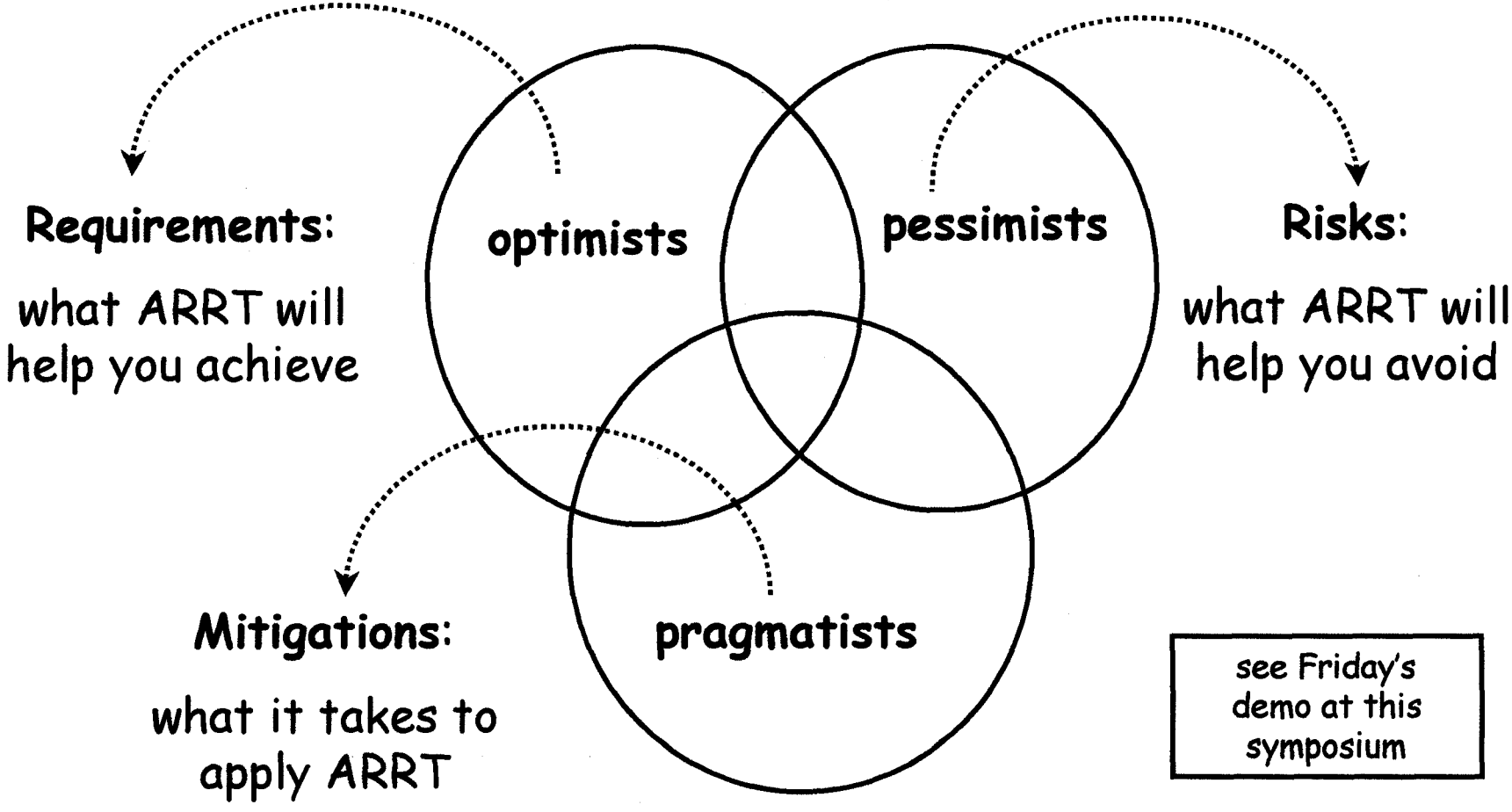
Shows issues, criteria of evaluation

Shows individual stakeholder perceptions/votes, group perceptions

Shows clusters spanning all criteria of an issue

Shows clusters per criterion, mean, max,min values

Concluding Remarks
even this talk maps to ARRT/DDP's concepts!



References

[Basili & Boehm, 2000] V. Basili & B.Boehm "CeBaSE: The Center for Empirically based Software Engineering" *NASA Goddard 25th Annual Software Engineering Workshop*, 2000.

[Cornford et al, 2001] S.L. Cornford, M.S. Feather & K.A. Hicks. "DDP - A tool for life-cycle risk management", *IEEE Aerospace Conference*, Big Sky, Montana, Mar 2001, pp. 441-451.

[Feather et al, 2000a] M.S. Feather, S.L. Cornford & M. Gibbel. "Scalable Mechanisms for Requirements Interaction Management", *4th IEEE International Conference on Requirements Engineering*, Schaumburg, Illinois: 119-129, June 2000.

[Feather et al, 2000b] M.S. Feather, S.L. Cornford & T.W. Larson. "Combining the Best Attributes of Qualitative and Quantitative Risk Management Tool Support", *15th IEEE International Conference on Automated Software Engineering*, Grenoble, France: 309-312, September 2000.

References

[Graves et al, 1998] T. Graves, M. Harrold, J. Kim, A. Porter and G. Rothermel. "An Empirical Study of Regression Test Selection Techniques". *20th Int. Conference on Software Engineering*, 1998, pp. 267-273.

[Greenfield, 1998] M.A. Greenfield "Risk Management 'Risk As A Resource' " *http://www.hq.nasa.gov/office/codeq/risk/*

[Hoh & Roy, 2001] H. In & S. Roy "Visualization Issues for Software Requirements Negotiation" *25th Annual International Computer Software and Applications Conference*, Chicago, IL, Oct. 2001.

[McGarry et al, 1998] F. McGarry, S. Burke & B. Decker. Measuring the impacts individual process maturity attributes have on software products., *5th International Software Metrics Symposium*, 1998, pp. 52-60